STATEMENT OF BETHANN ROONEY
MANAGER, PORT SECURITY
PORT COMMERCE DEPARTMENT
THE PORT AUTHORITY OF NEW YORK & NEW JERSEY

ON MEETING THE CHALLENGES OF PORT SECURITY
INFORMATION SHARING

BEFORE
US HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, FINANCE AND ACCOUNTABILITY

BROOKLYN, NEW YORK
JULY 10, 2006

Chairman Platts, Ranking Member Towns, members of the Committee, thank you for the opportunity to testify on the important issue of homeland security as it relates to our nation's ports. I am Bethann Rooney and I am the Manager of Port Security at the Port Authority of New York & New Jersey.

I appreciate the invitation to speak on port security and the steps that we have taken since 9/11 to secure our ports and maritime industry from terrorist acts and how federal initiatives like the Maritime Transportation Security Act (MTSA) of 2002 are positively impacting port security. The tragic events of September 11th have focused our collective attention on the need to protect our borders at major international gateways like the Port of New York and New Jersey and small ports alike.

This morning I would like to discuss four key points: 1) the vital nature of our ports and Maritime Transportation System; 2) the terrorist risk to those ports; 3) what we have done since 9/11 to address that risk with special focus on the area of information sharing; and finally 4) what the Committees can do to help us.

THE VITAL NATURE OF PORTS

Ninety-five percent of the international goods that come into the country come in through our nation's 361 ports; twelve percent of that volume is handled in the Port of New York and New Jersey alone, the third largest port in the country. The Port generates 232,900 jobs and $12.6 billion in wages throughout the region. Additionally, the Port contributes $2.1 billion to state and local tax revenues and $24.4 billion to the US Gross National Product. Cargo that is handled in the Port is valued at over $132 billion and serves 80 million people, or thirty five percent of the entire US population. In 2005 the port handled over 5,300 ship calls, 4.792 million twenty-foot equivalent units (TEU's) or 2.8 million containers, which is approximately 7,600 containers each day, 722,411 autos and 85 million tons of general cargo. Today international trade accounts for 30 percent of the US economy. Considering all this, it is easy to see how a terrorist incident in our nation's ports would have a devastating effect on our country and its economy.

THE TERRORIST RISK

When describing the potential impact of a terrorist event, the words "risk", "threat" and "vulnerability" have generally been used interchangeably. The fact however is that in the standard risk equation, risk is a factor of threat, vulnerability and consequence. Therefore, any discussion of the terrorist risk to ports must include each of those three areas.

The most difficult concept to understand is threat, mostly because it is a moving target and terrorists are devising new tactics everyday. There are however a number of threat concerns that are believed to be more likely and therefore are the ones that most maritime security programs today are built around. These include the use of ports or vessels as a means to smuggle weapons of mass destruction or terrorist operatives into the United States, the use of ships as a weapon to attack critical infrastructure, the scuttling of ships in major shipping channels and terrorist attacks on ships such as ferries or oil tankers. Since 9/11, we have seen a number of these tactics used around the globe with events such as suicide bombings using containers in the Port of Ashdod, small boat attacks on an

oil platform in Al Basra and the French oil tanker Limberg, and the transportation of suspected terrorist operatives via containers in Italy.

The maritime transportation system's vulnerability or the likelihood that the safeguards will fail is complicated by the general nature and openness of ports, with hundreds of miles of shorelines and facilities that have historically been public access areas. Additionally, the movement of cargo has been built on the tenets of speed, reliability and cost, not security. Therefore, the sheer volume of containers that move through US ports on a daily basis makes them each one of them a potential Trojan Horse.

The consequences of a terrorist attack by means of the maritime industry would have an overwhelming and lasting effect. Not only could there be significant death and destruction but the national and global economies would be devastated. It is estimated that for every day that a port is shut down, it takes seven days for recovery. As evidenced by with West Coast labor strikes last year, a ten-day shut down is estimated to have cost one billion dollars a day.

While we can't do anything to address the threat, we can use our understanding of the threat, to make infrastructure improvements, and create policies, programs and procedures that can help reduce our vulnerability and consequences to mitigate our overall risk.

OUR PROGRESS SINCE 9/11

As a result of significant legislative action, capital investments and operational improvements on the part of the public and private sectors in the nearly four and a half years since 9/11, the Maritime Transportation System (MTS) is more secure today than ever before. While significant progress has been made and much has been accomplished, work still remains to be done.

<u>A Multifaceted Approach</u>

Enhancing maritime security is a complex problem, which requires a multi faceted and layered approach. Maritime security is so much more than just the physical security of our ports and terminals and the vessels that use them, we must also enhance cargo and supply chain security. Furthermore, while much of the focus in on preventing another terrorist attack; we must also work on developing comprehensive programs that address not only prevention but awareness, response, consequence management and business recovery as well. This requires the full participation and cooperation of the federal, state and local government as well as the private sector and our international partners.

Roles and Responsibilities

While there are dozens of federal, state and local agencies and private sector partners that share responsibility for port security, the primary players are the United States Coast Guard (USCG), the Bureau of Customs and Border Protection (CBP) and vessel and terminal operators. The USCG is the lead federal agency for maritime security. As such, the Coast Guard is responsible for security of our nation's channels and waterways and enforces the Maritime Transportation Security Act of 2002, which all vessels and port facilities must comply with. The Coast Guard has a number of programs and initiatives in their toolbox to uphold their maritime security mission. CBP is the lead federal agency for cargo security. As such, CBP administers a number of cargo security regulations and programs including the 24 Hour Rule, the Automated Targeting System (ATS), various Non Intrusive Inspection equipment, the Customs Trade Partnership Against Terrorism (C-TPAT) and Container Security Initiatives (CSI) among other things. Each of the terminal and vessel operators are required to comply with federal security regulations and operate in accordance with their USCG approved Facility and Vessel Security Plans. The terminal operators also coordinate and cooperate with the USCG and CBP on their various security programs.

Physical Security

The Maritime Transportation Security Act of 2002 or MTSA and the implementing regulations are a groundbreaking development in the area of port, terminal and vessel

security. Effective July 1, 2004, the MTSA required that security assessments be conducted, security plans written and adhered to, security officers appointed and all personnel trained in security. In most cases, compliance required an investment in physical infrastructure as well as operational adjustments.

There are 197 regulated facilities here within the Captain of the Port zone. Of those 197 facilities, just 13 of them are located on Port Authority property. While they may be located on Port Authority property, by regulation, the facility operators such as American Stevedoring, Inc. at the Red Hook Container Terminal here in Brooklyn and New York Container Terminal, Inc. at Howland Hook in Staten Island are responsible for compliance with the regulations. Although the Port Authority is responsible for law enforcement and emergency response at all of our port facilities, under MTSA we are only responsible for the security at our public berths and other critical infrastructure at the port facilities such as the roadways and utilities.

Multi Agency Coordination

Good security is not merely a function of what you do within your fence line but rather a factor of what neighboring facilities are doing, or not doing, and how the public sector works with you to develop your security program. Immediately after 9/11, the Port Authority formed two committees in order to facilitate the exchange of critical security information and best practices between and among our customers and the federal, state and local law enforcement and emergency response communities that serve them. The Tenant Security Working Group meets a minimum of monthly, and more often as the threat level increases. This Working Group provides a forum for port users to exchange lessons learned, share best practices, develop programs and solicit feedback from the federal, state and local government partners on issues of concern. This environment ensures that port security is not a competitive issue but rather an all hands evolution.

Similar to the Tenant Security Working Group, the Port Authority also sponsors a Law Enforcement Security Committee. The Law Enforcement Committee brings together the

approximately 25 federal, state and local law enforcement and emergency response agencies that have responsibilities within the port region. Also held monthly or as often as the threat dictates, this forum provides an opportunity for the exchange of intelligence, discussion about discrete security programs and initiatives, and planning of drills, exercises and training.

In addition to these two forums that the Port Authority sponsors for our facilities, the Coast Guard heads up an Area Maritime Security Committee (AMSC), the objective of which is to continually assess security risks to the ports, determine appropriate risk mitigation strategies, and develop, revise, and implement the AMS Plan. The AMSC also serves as a mechanism by which security threats and changes in MARSEC Levels are communicated to port stakeholders.

The relationships that have been established through a variety of real life situations such as the CSAV Rio Puelo, the "lemon ship" that called in our Port in the summer of 2004 are fostered and further developed through these committees and have been beneficial in preparing for our response to and recovery from future incidents. Just as the Department of Homeland Security has "One Team and One Fight" so too do the partners in the Port of New York and New Jersey.

Cargo and Supply Chain Security

America's consumer-driven market now depends upon a very efficient logistics chain, of which the nation's ports are just a single link. US ports provide the platform to transfer imported goods from ships to our national transportation system—primarily trucks and trains—that ultimately deliver those products to local retail outlets or raw goods to manufacturing plants. Historically, that goods movement system has had one overall objective: to move cargo as quickly and cheaply as possible from point to point. Today, a new imperative —national security—is imposing itself onto that system. As such, we know that ports themselves are not the lone point of vulnerability. Rather, the potential

for terrorist activity stretches from where cargo is stuffed into a container overseas to any point along the cargo's route to its ultimate destination.

Our goal should be to increase our confidence that we know exactly what is in each container *before* it is off loaded in a US port. It is not possible to physically examine the contents of each of the 7,600 containers that arrive each day in the Port of New York and New Jersey. The key is finding a way of separating high-risk cargoes from the vast majority of legitimate containers and then dealing with the exceptions. This approach requires a systematic understanding of the logistics chain that now moves that container from any place in the world to the distribution system in our country.

A typical container movement includes 14 different nodes and 30 organizations, and generates from 30-40 different documents with over 200 data elements. This is a complex process but the physical movement of a container is only one dimension of the system. There are three other components that must be understood. There is the flow of money, the flow of information and data on the shipment, and, finally, the transfer of accountability that all must occur in order for the cargo to be delivered.

Today, there are no mandatory security standards when loading a container at the manufacturer or consolidated in a warehouse, often well inland of a seaport. There are no security standards for the seals that are put on containers. Cargo is transferred from one mode of conveyance to another and there are neither standards for how that is done nor accountability for the integrity of the container as it changes hands.

We believe that efforts must be taken to verify the contents of containers before they are even loaded on a ship destined for a US port. The process must include certification that the container was packed in a secure environment, sealed so that its contents cannot be tampered with, and transported under the control of responsible parties. A chain of custody must be established that ensures the cargo's integrity and requires that complete and accurate data be provided to Customs well in advance of a ship's arrival in the United States.

The many programs that the Bureau of Customs and Border Protection have implemented in the last four years—the 24-Hour Rule, the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), the increase in Non-intrusive Inspection (NII) exams and the deployment of Radiation Portal Monitors (RPM's) at terminals are all valuable elements of a layered security system and must be supported with the necessary resources and funding.

Operation Safe Commerce (OSC)

We believe however that a program like C-TPAT should not be voluntary but rather minimum supply chain security standards should be required of each party in the supply chain. To demonstrate the validity of this view, the Port Authority of New York and New Jersey, in cooperation with the Department of Homeland Security Office of Grants and Training (OGT), state agencies and numerous private sector partners, is participating in an initiative called Operation Safe Commerce (OSC). OSC is a public – private partnership that responds to the twin imperatives of facilitating legitimate international commerce and increasing security while minimizing the impact on commerce. The goal is to develop dependable arrangements for verifying, securing, monitoring and sharing information about cargo from the point of origin, throughout the supply chain, to its final destination. This will be accomplished through the identification and evaluation of new technology, business processes, policies and procedures that could improve supply chain security, and minimize disruption to commerce. The solutions must also be economically and commercially viable. Private companies have volunteered to join with us to construct prototypes of a secure international supply chain.

We believe that the ideal system would allow us to:

- Know ahead of time that the container is free of false compartments;
- Have assurances that the cargo and shipper are legitimate and that reasonable care and due diligence have been used in packing, securing, and manifesting the goods in a container;

- Verify at any point along the route that neither the container nor the cargo has been tampered with; and,
- Verify that the integrity of the information and information systems associated with the movement of the cargo has not been compromised.

The first phase of OSC for which the Port Authority received $13.8 million was completed in November 2004. We studied a total of 155 containers across six supply chains and evaluated such things as electronic seals, radio frequency identification tags, indicative tape, chemical, biological and radiation detection devices, third party inspection companies, and employee training.

Unfortunately, the OSC findings and recommendations are considered Sensitive Security Information (SSI) and I am not at liberty to discuss them in a public forum such as this. I will however say that we identified some very promising and cost effective solutions and generally found that supply chain partners are eager to increase security in their operations. In most cases, however, they are hesitant to make any investment until final regulations are promulgated.

In April 2005, we received an additional $5.2 million to conduct important follow on work to OSC, which includes more strenuous lab testing of the "best of breed" technologies from OSC Phase II and a longer deployment test phase using a high volume of containers. We are currently monitoring the status containers that are moving from Europe and the Middle East to the Port of New York and New Jersey with a Container Security Device (CSD) that has a number of sensors capable of detecting various types of security breaches or risks When the testing concludes in October 2006, it is our collective hope that we can provide constructive and tested recommendations on how to secure the supply chain without burdening commerce with unnecessary costs or delays to the detriment of our region and the national economy that could be implemented by the federal government and the International Maritime Organization.

Operation Safe Commerce is just one of numerous federally and privately funded supply chain security projects that are currently underway. While many of these individual projects show great promise, true progress and results are hampered by the fact that they are not tracked, managed and coordinated by a single Department or Agency and as a result lessons learned are not being shared, results are not being leveraged and funds are being wasted. We believe that all cargo security research and development projects should be managed by a single organization within DHS that acts as the central repository and clearing house for all studies and the focal point on supply chain security issues.

Radiation Test Bed

As yet another line of defense, the Port Authority has been working with the Department of Homeland Security on a very productive program of testing radiation sensor technologies at locations at our river crossings, aviation and port facilities including the New York Container Terminal on Staten Island. Our facilities are being used as a test-bed to see how the various technologies and products operate in environments like tunnel portals and on the waterfront. We hope to build expand the test-bed operations to increase radiation sensor coverage at the region's critical infrastructure and to advance the capacity of technology to be reliable and of practical use.

Communications and Information Sharing

One of the principal outcomes of the work of the 9/11 Commission was the determination that information sharing and collaboration at all levels of government were less than adequate.

While we support the implementation of regional or port-wide Joint Operations Centers, we do not support the development of operations centers exclusively for maritime and cargo security as currently outlined in the proposed legislation. The maritime industry does not operate in a vacuum but rather is largely dependent on surface transportation (road and rail) and requires the involvement of multiple levels of government and public safety agencies. Each of these agencies have information networks and operations centers of their own that must be staffed and supported which are expensive to maintain

in both personnel and infrastructure. A new port Joint Operations Center would require personnel from agencies already stretched to the limit. Therefore, any new Joint Operations Center created through future legislation should not be limited to maritime and cargo security alone but be a single focal point and provide for the integration of all Homeland Security related functions among local, state and Federal agencies in a given region. It must also not just be a single center but a coordinating node in a regional and national information sharing and collaboration network linked to other operations centers.

Over the last several years, hundreds of millions of dollars in Federal Homeland Security funding has been spent to develop and implement disparate information sharing networks and joint operations centers at the local, state and federal levels without the benefit of a coherent federal vision on a national homeland security architecture. Absent such a vision and a set of guiding standards, we run the significant risk of local, state and federal operations centers that need to work together in an emergency not being compatible with one another in technology, operational methods or both.

There are three promising efforts now underway that we recommend Congress consider. The first is the National Command Capability Working Group, a Joint DHS / DoD program to set direction for a national information sharing and collaboration network. The second is a program called Joint CONUS Communications Support Enterprise (or JCCSE), a joint project of US Northern Command and the National Guard Bureau. The third effort is the Regional Information Joint Awareness Network or RIJAN. RIJAN is a DHS funded, DoD managed and Port Authority led multi-agency project to build an information sharing and collaboration network among key operations centers in the New York and New Jersey port region. Regional partners include the States of New York and New Jersey and the City of New York. DHS sponsorship is via the Domestic Nuclear Detection Office (DNDO). Our DoD program manager and developer is the US Army's Communication Electronics Development and Engineering Command from Fort Monmouth New Jersey.

Although the creation of formal Joint Operations Centers in ports around the country is still in the earliest stages of discussion, there are other initiatives and activities underway to help improve information sharing among stakeholders. The most significant of these initiatives is the creation of Area Maritime Security Committees (AMSC) that were required to be established in each port under the Maritime Transportation Security Act of 2002. While the structure and function of these committees varies from port to port, by and large they facilitate coordinated planning and the exchange of information among various port stakeholders. The AMSC here in the Port of New York and New Jersey is made up of over 40 federal, state, local and private organizations that have a stake in port security. Executive leadership from each of these organizations get together on a monthly basis to coordinate port wide activities and initiatives, receive intelligence briefings and help the Captain of the Port develop security policies and procedures.

In the past month, the AMSC completed the development of a 2 Year Strategic Plan and a structural reorganization to ensure that we are able to address the myriad of goals and objectives that were identified in the Strategic Plan. The AMSC is organized into six sub committees as follows: Communications, Planning & Preparedness, Response & Recovery, Intelligence, Training & Exercises and Grants & Legislative Activities. There are a number of initiatives that the Communications Sub Committee will be working on in the next two years including maximizing the use of the Coast Guard's Homeport Website and the 3N Notification System. Both of these systems have helped to vastly improve communications with the private sector players, wherein hundreds of entities can be simultaneously informed of breaking news and important information.

While it has not been an issue yet in the Port of New York and New Jersey, the lack of proper security clearances for key state, local and private sector stakeholders has the potential to be a significant barrier to an effective response to a credible security threat. The AMSC was allocated just 10 security clearances in early 2005. That's 10 security clearances for the second highest risk port in the Nation. In the event of a credible threat, there is no way to communicate above the Sensitive Security Information (SSI) level to many of the AMSC Executive Members and the vast majority of the 197 Facility Security

Officers in the Port. Congress and the Administration must find a way to expedite the processing of security clearances, especially for those individuals that have previously held clearances and to cross honor clearances that were issued by another Department or Agency.

FEDERAL FUNDING

Clearly there is an on going debate over whether port security is a federal government or private sector responsibility. While that debate continues, the Port Authority and private terminal operators throughout the country have willingly taken significant steps to protect our seaports from the new terrorism threat, because the consequences of not doing so are grave. Since September 11th, ports such as ours have instituted heightened security measures and spent significant amounts of money to increase security, both with capital improvements and additional security and law enforcement personnel. However, for every dollar that is spent on security, there are ten fewer dollars that can be spent on the capital infrastructure that is required to accommodate the increasing volume of cargo that our ports are expected to handle.

In an attempt to provide you with a sense of the scope of the challenge we face, I offer two possible indicators of local port needs.

Since June 2002 when the first round of Port Security Grants was made available, terminals in the Port of New York and New Jersey have applied for over two hundred million in Federal assistance. Of the $707 million that has been appropriated for port security grants across the country, a total of $53.7 million, which is just 7.5 percent of the total, has been awarded to entities in our Port. The Port Authority alone has submitted requests totaling $42 million, but has been awarded only $10.5 million, including $2.3 million for technology demonstration projects which the Port Authority sponsored on behalf of the federal government, or twenty five percent of the identified need.

In the Coast Guard rulemaking, they estimated that the cost for port facilities throughout the country to implement the MTSA over the next decade would be $5.4 billion. Given the required cost share for federal grants of twenty–five percent, by the Coast Guard's own estimate, it would require $400 million a year in federal assistance in order for ports and terminals to adhere to the MTSA. Despite this, only $175 million was allocated nationwide for port security in FY 2006. That is significantly more than was requested in the President's budget, but still far short of the need that America's ports have identified.

While these grants help defray that cost of physical security measures, such as access control, intrusion detection, fencing, lighting, identification systems, CCTV and gates, there has also been a significant increase in the operational costs associated with maritime security as well. It is estimated that the annual operations and maintenance costs associated with the new security systems is on the order of magnitude of fifteen to twenty percent of the purchase price. Additionally, ports and terminals have spent significant sums of money on personnel related costs, including the hiring of new security officers, overtime, upgrading security forces to use more professional services and for providing extra training. The Port Authority's port security operating costs have doubled since 9/11. This does not include the extra police that are required at all Port Authority facilities every time the threat level increases, which amounts to approximately $500,000 per week.

WHAT CAN THE COMMITTEES DO TO HELP?

Chairman Platts, the attacks of September 11th were not directed at a maritime facility, but those terrible events provided the impetus to focus attention on our marine transportation system, which is so essential to our national economy and defense. You and your committee are to be commended for bringing focus to such a daunting task.

As the Committee moves forward this year, we would ask that you:

1) Accept an open invitation from the Port Authority to the Committee members and your staff to visit the port and become more educated about our issues and concerns;

2) Use your influence to promote such issues as the development of multi modal Joint Operations Centers, the allocation and expedient processing of security clearance and the imperative for supply chain security standards.
3) Support legislation that would give the federal agencies that are responsible for port security the resources they need to do their important jobs.

Addressing the issue of port and maritime security is an enormous challenge given the complexity of the international transportation network. Devising a system that enhances our national security while allowing the continued free flow of legitimate cargo through our ports will not be solved with a single answer, a single piece of legislation, or by a single nation. It will require a comprehensive approach with coordination across state lines and among agencies of all levels of government and the cooperation of the private and public sectors and the international community. Importantly, it will require additional resources for the agencies charged with this awesome responsibility and for the public and private ports and terminals where the nation's international commerce takes place.

I hope my comments today have provided with you some helpful insight on this complex matter. We at the Port Authority of New York & New Jersey are prepared to offer any additional assistance that you may require. Thank you.